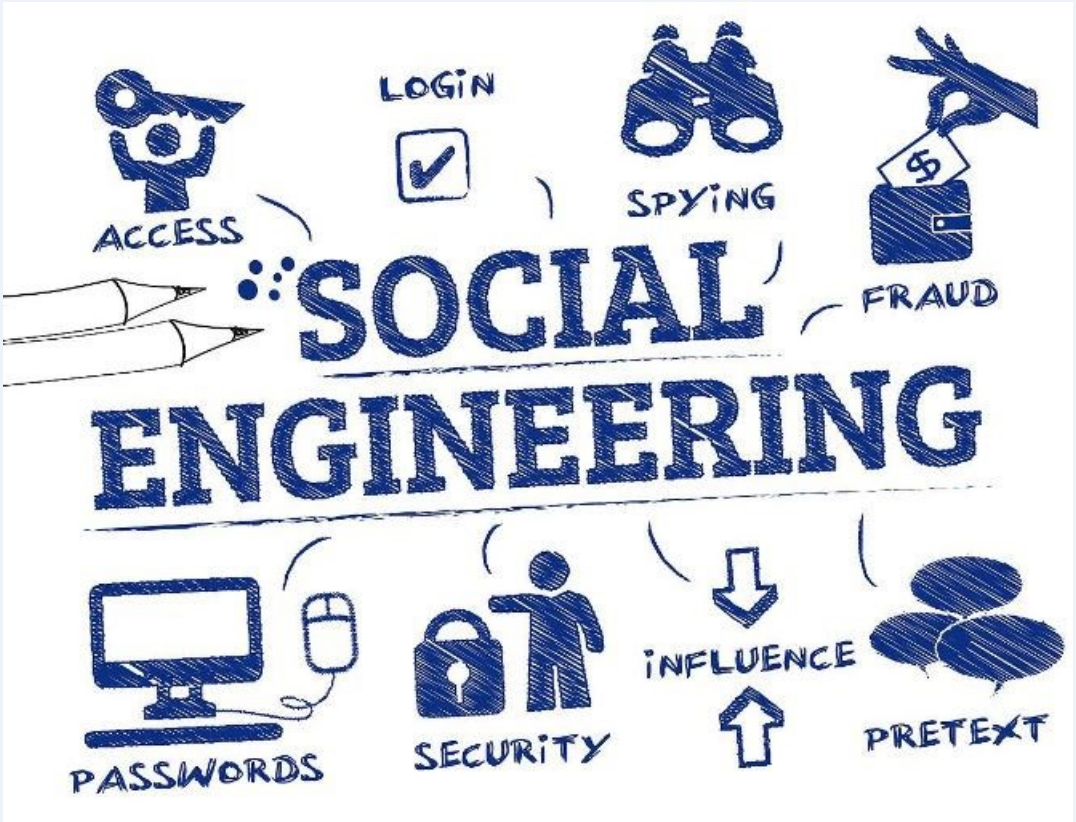
NEWS
Cyber Security
Vol. 3 | Issue 5 May 2018

Hello everyone and welcome to this month's TXDPS Cyber Newsletter.

Hopefully everyone survived tax season relatively unscathed without owing anything or falling victim to any scams. This month I found a few articles which I believe you will find interesting and hopefully useful. For the month's "theme" I decided to focus on the dangers of Social Engineering and the Internet of Things (IoT). The dangers of Social Engineering to the Agency cannot be stressed enough. It is a danger anyone can fall victim to and must be ever vigilant to defend against. The other theme, Internet of Things, could be a danger not only to the Agency but it is an even greater danger to you personally. Hopefully this month's articles will educate you on some topics you were not aware of as well as pique your interest to learn more.

I have added a new section to the newsletter; Reader Suggestions. The section, as the name implies, will be dedicated to articles of interest employees send me. My hope is that for all future newsletters I will have multiple articles or topics to post. If you have a suggestion or come across an interesting article, please let me know.



Cyber News!!

North Korea-linked hackers stole data from 17 countries in an ongoing cyberattack that's far bigger than we thought

A North Korea-linked hacking group has been tied to a series of cyberattacks spanning 17 countries, far larger than initially thought.

A new report by McAfee Advanced Threat Research found a major hacking campaign, dubbed Operation GhostSecret, sought to steal sensitive data from a wide range of industries including critical infrastructure, entertainment, finance, healthcare, and telecommunications.

Attackers used tools and malware programs associated with the North Korea-sponsored cyber unit Hidden Cobra, also known as Lazarus, to execute the highly sophisticated operation.

Click **HERE** to read more.

Old Worm, New Tricks: FacexWorm Targets Crypto Platforms

Malicious Chrome extension FacexWorm has reappeared with new capabilities, targeting cryptocurrency platforms and lifting user data.

FacexWorm, a malicious Chrome extension, has been rediscovered targeting cryptocurrency trading platforms and spreading via Facebook Messenger. The Cyber Safety Solutions team at Trend Micro reports it's packing a few new capabilities, including the ability to steal user data.

The extension was first detected in August 2017 and returned the following April amid reports of increased appearances in Germany, Tunisia, Japan, Taiwan, South Korea, and Spain. Like the original, it sends socially-engineered links to friends of affected Facebook account holders.

Click **HERE** to read more.

A malicious USB stick could crash your Windows PC, even if it's locked

Plugging a USB drive containing a malformed NTFS image into a Windows machine can cause it to bluescreen in mere seconds, according to Marius Tivadar of BitDefender.

Tivadar recently published his NTFS image on GitHub after dissatisfaction with Microsoft's response. He initially reported the bug in July 2017, and "they did not want to assign CVE for it nor even to write me when they fixed it," Tivadar said.

Microsoft replied to Tivadar, saying "Your report requires either physical access or social engineering, and as such, does not meet the bar for servicing down-level (issuing a security patch)."

Attempts to test the code have had varying results, with one commenter on Bleeping Computer saying the bug doesn't work as Tivadar claims. Whether or not Tivadar's code is as effective as he said it is doesn't matter, as another Bleeping Computer commenter said.

Click **HERE** to read more.

More Cyber News!!

Why Hackers Love Healthcare

The migration of valuable data to the cloud is piquing the interest of cybercriminals. But there are ways to fight back.

Much like the rest of the world, healthcare organizations are shifting work to cloud services in order to improve accessibility and patient care. However, the migration of these workloads and moving valuable information such as PHI (personal health information) and PII (personally identifiable information) to the cloud has also led to cybercriminals taking a particular interest in the industry.

The number of ransomware and other malware attacks is rising incredibly fast in the healthcare industry, putting human lives as well as critical data at risk. From 2011 through 2014, the sector—including hospitals, labs, pharmacies, drug companies and outpatient clinics—experienced the highest number of data breaches of all industries. What makes these organizations such a popular target?

Click **HERE** to read more.

Vade Secure Discovers New Phishing Attack Targeting 550 Million Email Users Globally

Vade Secure has discovered a new phishing attack that represents more than 550 million emails sent since Q1 2018. First detected in early January, the phishing attack is targeting consumers around the world. Countries with high concentrations of impacted email users include the US, UK, France, Germany, and the Netherlands.

The phishing attack attempts to steal users' bank account details by offering them a coupon or discount in exchange for participating in a quiz or online contest. The emails masquerade as popular brands, online streaming services, and telecom operators based on the country of the recipients. Examples include Canada Pharmacy in the US, as well as Orange and Carrefour in France. Moreover, the content of the messages is adapted according to the local language.

Click **HERE** to read more.

More Cyber News!!

Getting an Amazon Echo app to silently eavesdrop on you

In news that will surely be a surprise to nobody, apps that run on Amazon's home assistant, Echo, can be turned into silent eavesdroppers: no fancy hacking required, no new Echo vulnerability pried open.

Or at least they could, until Amazon fixed it.

Researchers at information security firm Checkmarx demonstrated what we probably all suspected was possible but hoped wasn't by tweaking options in Alexa's software development kit (SDK) – the kit that's used to develop software, known as skills, for the Echo.

The voice-activated skills are the equivalent of the apps on your phone: discreet bits of software that add capabilities to the device. There are skills for finding open restaurants near you, getting Starbucks started on your coffee order, checking your bank balance, hearing the latest news and turning on the Christmas lights.

And on somebody's desk at Checkmarx, there's one for eavesdropping on you. It silently captures transcripts of what you're saying and sends them to an external log accessible to the researchers who rigged the trap.

Click **HERE** to read more.

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

LONDON - Hackers are increasingly targeting "internet of things" devices to access corporate systems, using things like CCTV cameras or air-conditioning units, according to the CEO of a cybersecurity firm.

The internet of things refers to devices hooked up to the internet, and it has expanded to include everything from household appliances to widgets in power plants.

Nicole Eagan, the CEO of Darktrace, told the WDJ CEO Council Conference in London on Thursday: "There's a lot of internet-of-things devices, everything from thermostats, refrigeration systems, HVAC systems, to people who bring in the Alexa devices into the offices. There's just a lot of IoT. It expands the attack surface, and most of this isn't covered by traditional defenses.

Click **HERE** to read more.

Reader Suggestions

As you can see, I have added a new section to the newsletter. This section will be dedicated to articles of interest that employees send me. This month's submission is from the DPS **CJIS Department**. The article is from News Channel 10 in Lubbock and is about a homeless man who used Social Engineering skills to convince a dispatcher in Lubbock to run license plates for him. The article is short so I will just post the whole thing.

LUBBOCK, TX (KCBD) - According to the police report, 58-year-old Eliseo Benites, a homeless man from Lubbock, has been indicted by a Lubbock County Grand Jury on charges of impersonating a public servant.

Eliseo Benites (Source: Lubbock County Detention Center)

According to the police report, Benites pretended to be a police officer in order to get license plate information. The police report also says Benites was successful in getting information for at least one license plate.

Benites called the police department on at least three occasions and possibly more, according to the report.

The indictment says Benites called the Lubbock Police Department dispatch for the information.

He is being held in the Lubbock County Detention Center on bonds totaling more than $20,000.

The actual article can be found **HERE**.

Social Engineering is a non-technical cyber danger. In very basic terms it is the psychological hacking of a human and is often the first step hackers take in the reconnaissance phase before an attack. The techniques used in Social Engineering are very similar to techniques investigators, interrogators, and sales/marketing people use to do their jobs. I could spend lots of time explaining how this is done but seeing is often the best teacher. Please watch the following links when you get a chance to see just how this is done.

Professional Social Engineer & Scammer

Social Engineering Fraud

Social Engineering for Fun and Profit

David Kennedy

Simple Social Engineering

Social Engineering: The Gentleman Thief

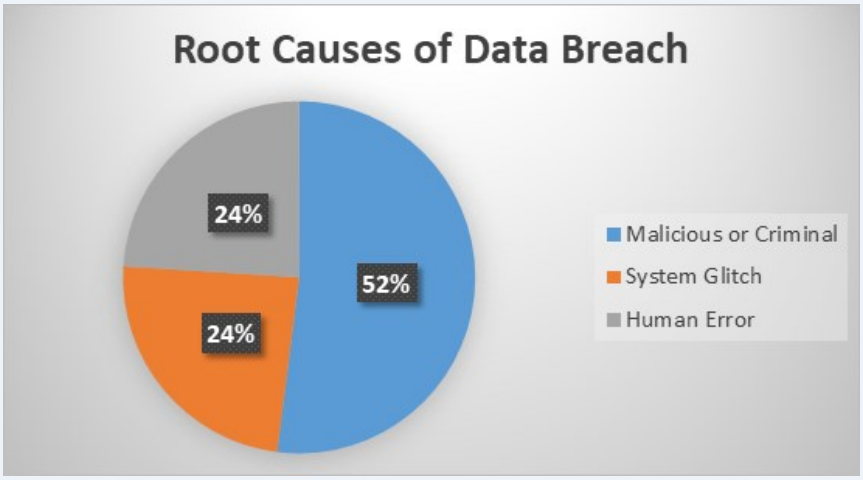
You can also go to this Agency internal link to see a PowerPoint presentation about the topic. Go down to slide 54 to learn more about Social Engineering.

Please send me any articles you think would be of interest to be added into the monthly newsletter. Email me at kirk.burns@dps.texas.gov.

<Cyber Stats for Mar and Apr>

	March 2018	% Change	April 2018
Phishing attacks against agency	17	17.65%	20
Emails blocked by sensors	Pending Code	100.00%	125,700
DPS Custom Email Threat Signatures Created	2	850.00%	19
Cyber Security	122% increase in the number of IOCs being tracked		

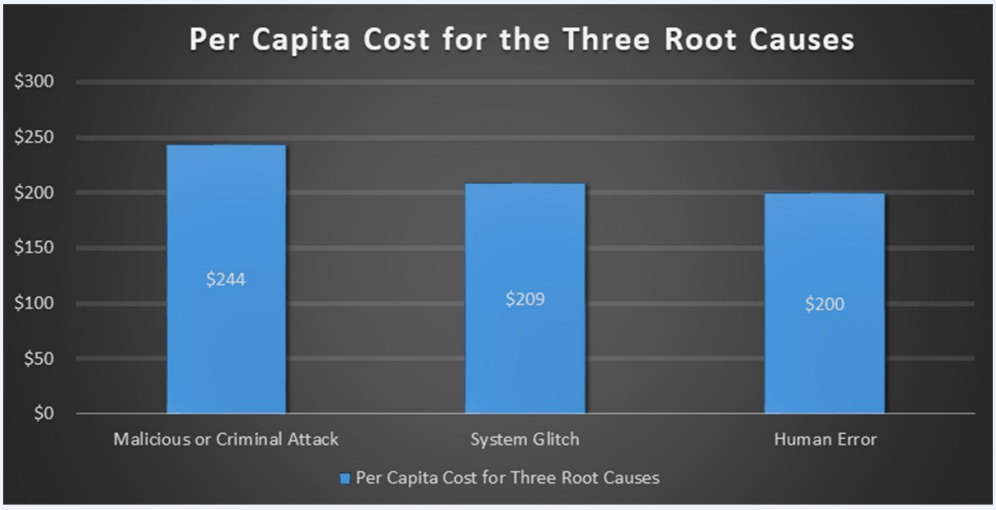
As you can see from this month's stats, phishing attacks against the agency have slightly risen from last month. The chart also shows a significant increase in Custom Email Threat Signatures and Incidents of Compromise (IOC). Even though the numbers are higher, it doesn't mean we are being targeted any more than normal. Attacks will fluctuate and the numbers only indicate just how good a job our Cyber Ops and IT teams are doing to protect the agency.



For this month's stats I would also like to include some information one of our new team members (**Dylan**) found in an independent study commissioned by IBM and published last year (2017). They found the following results (see graphs).

There are a few things I would like you to take away from these graphs. First is that 52% of all data breaches are from malicious attacks, but almost 1/4 (24%) were from human error. The second is the cost of these data breaches. While malicious attacks were more costly, human error isn't far behind and can be seen in the graph below. As you can see, the dollar differences per document between the root causes of a breach are negligible. Unsurprisingly, it was also found the longer a breach went undetected the more costly it was. Breaches found under 100 days had a average cost associated with them of $5.99 million while those longer than 100 days rose to $8.7 million.

Data Breaches also take a significant amount of time, and resources to recover from. Not to mention the amount of lost revenue and eroding of customer confidence in the organization. In their study, IBM found 45% of the cost of data breaches is from lost customer business with the next most costly being Legal at 19% and Investigations and Forensics being 18%.



Cyber Challenge

This month's Cyber Challenge is more of an awareness challenge. I am going to challenge you to take a look at the world around you and see how many devices are now connected to the internet. I think it will surprise you just how many common things are now being attached to the Internet. For example, the fish tank thermometer mentioned in one of this month's articles.

Recently I came across an IoT device that shocked me. Your eyes are not deceiving you. You really are seeing a BBQ Grill that can be attached to your network. I saw it at the Bucky's in Bastrop last month. While I have not researched it, I'm willing to bet the manufacturer has no plan for updates to the grill if vulnerabilities are found. To help you on your path with the awareness challenge, here are some common things that are online you may or may not know about.

Tablets, smart phones, smart TVs, refrigerators, home thermostats, home assistance (Echo, Alexa, etc), doorbell cams, home air quality sensors, WeMo, security systems, security cameras, baby monitors, garage door openers, crockpots, ovens, dishwashers, washers and dryers, water heaters, home automation, coffee pots, NEST, lights, light bulbs, smoke detectors, the batteries in smoke detectors, etc.

I challenge everyone to think about what malicious things could be done to and with the devices you find. Is it really necessary to have a smoke detector's battery be able to notify you via an app that it needs to be changed? And does the manufacturer routinely update their product to help keep your network safe? If not, are you willing to accept the RISK of having these devices on your (or any) network?

Kirk